1 Teória vypočítateľnosti – poznámky z prednášky #1

1.1 Zobrazenia a funkcie

Definícia. Čiastočné (totálne) zobrazenie trojice (A, B, f) pre ktoré platí:

- $f \subseteq A \times B$
- Ku každému vstupu $a \in A$ existuje najviac jeden (práve jeden) $b \in B$ taký, že $(a, b) \in f$.

V takom prípade píšeme $f : A \to B$.

Poznámka. Ak je zobrazenie totálne, tak je aj čiastočné.

Označenie. A sú vstupy, B sú výstupy, f je graf.

Pozor! $f : N^K \to N$ je funkcia (N^K, N, f). V takomto prípade sa budeme tváriť, že f má viac parametrov, aby tam neboli zátvorky:-), čiže $f \subseteq N^K \times N$. Jednoznačnosť sa zapíše analogicky `:-P`.

Definícia. Rovnosť medzi dvomi výrazmi chápeme nasledovne: $A = B$ – buď sú obidvaja definovaní a majú rovnakú hodnotu, alebo sú obaja nedefinovaní.

Definícia. $Arg(f) = \{x_1, \dots, x_k | \exists y : (x_1, \dots, x_k, y) \in f\}$
$Val(f) = \{y | \exists x_1, \dots, x_k : (x_1, \dots, x_K, y) \in f\}$

Poznámka. Ak $Arg(f) = N^k$, TAK JE VŠADE DEFINOVANÁ (totálna), Ak $Arg(f) \subseteq N^K$, tak je čiastočná funkcia.

Definícia. Nech f, g sú čiastočné funkcie na A. Budeme hovoriť, že f je zúžením g alebo g je rozšírením g ak $f \subseteq g$. Ak g je rozšírením f, a g je totálna na A, potom budeme g nazývať zúplnením čiastočnej funkcie f na množine A.

Definícia. Nech $M \subseteq N^k$. $\chi(x_1, \dots, x_k) = 0$ ak $(x_1, \dots, x_k) \notin M$. $\chi(x_1, \dots, x_k) = 1$ ak $(x_1, \dots, x_k) \in M$. χ je charakteristická funkcia.

Definícia. $c\chi_M(x_1, \dots, x_n)$ je nedefinovaná, ak $x_1, \dots, x_n \notin M$. $c\chi_M(x_1, \dots, x_n) = 1$, ak $x_1, \dots, x_n \in M$.

Definícia. Ak $f(x_1, \cdot, x_n) \uparrow$ - nedefinované
$\downarrow$ - definované

1.2 A. Churchova λ notácia pre funnkcie $N^K \to N$.

Príklad.

- $\lambda xy \quad (5x + y)$.
- $\lambda xyz \quad (5x + y)$ – fiktívna premenná.
- $\lambda y \quad (5x + y)$ – x je parameter opisujúci množinu funkcií
- $\lambda y \quad (10)$ – unárna konštanta.
- $\lambda \quad (10)$ – nulárna konštanta.

Pozor! $\lambda xy \quad (x^3 + y) = \lambda yx \quad (y^3 + x)$
$\lambda xy \quad (x^3 + Y) \neq \lambda yx \quad (x^3 + y)$

1.3 Algoritmus a funkcia vypočítateľná algoritmom

Formalizácia: – text je prvok Σ^*. Nie hociktorý text je považovaný za algoritmus. Je potrebné mať nejakú podmienku, ktorá rozhoduje, či daný text je, alebo nie je textom opisujúcim algoritmus. Príkladom môže byť napríklad nejaký programovací jazyk. Podmienka musí byť algoritmicky rozhodnuteľná. V rámci formalizácii, budeme požadovať aj nejakú sémantiku – čo počíta. Ďalšia podmienka je, že daný algoritmus musí počítať funkciu jednej (k) premenných. Táto podmienka musí byť tiež algoritmicky riešiteľná.

Príklad. Extencionálnosť: Je rozdiel medzi funkciou a spôsobom jej zadania. Algoritmickú funkciu nemusíme zadať algoritmom, teda vieme mať zadanú funkciu ale nevedieť čo počíta. Preto sa budeme viac zaoberať zadaním.

$f(x) = 1$ ak v desiatkovom rozvoji čísla Π je presne x číslic 5 idúcich za sebou. Ináč $f(x) = 0$. Doteraz nikto nezistil, či existuje algoritmus, čo počíta túto funkciu.

$g(x) = 1$ ak v desiatkovom rozvoji Π je aspoň x číslic 5 idúcich za sebou. 0 ináč. Táto funkcia je "monotónna" – najskôr je to jedna, a potom nula alebo je to stále jedna. V oboch prípadoch je to to vypočítateľná funkcia (iba jeden if, alebo iba výpis 1). Ale neviem ktorý algoritmus je správny`;-P`

Domáca úloha 1.3.1 *Čo znamená extencionálnosť?*

1.4 Diagonalizácia totálnych funkcií

Chceme aby všetky intuitívne vypočítateľné funkcia boli v rámci formalizácie vypočítateľné. Snaha je postihnúť formalizmom všetky intuitívne algoritmicky vypočítateľné funkcie (toto sa ale nedá `:-/` .

Diagonalizácia pre funkcie jednej premennej umožňuje nájsť totálnu funkciu, ktorá nie je opísaná v rámci daného formalizmu. Máte generátor postupností, a z nich vyberieme syntakticky správne programy $(P_0, \ldots, P_m)$. Pre každý sa spýtame, či počíta funkciu jednej premennej. Teraz máme programy $(P_0, \ldots, P_s)$.

Program P_i počíta funkciu f_i.

Nech $h(x) = f_x(x) + 1$ – zmeníme hodnotu. Máme funkciu ktorá je rozdielna od každej. Je totálna aj intuitívne vypočítateľná. Ale naša formalizácia ju nezachytila. (presný dôkaz by bol sporom, ale nechce sa mi ho písať, kto chce, nech si domyslí, kto nevie, nech si doštuduje).

Toto nie je plne formalizované v zadefinovanom zmysle. ???

Formalizovať čiastočne definované funkcie: – nestane sa nám problém s diagonalizáciou – niekde to nie je definované, tam +1 nebude definované, a teda sa to bude podľa definície rovnať.

Veta 1.4.1 *Existuje presne $\aleph_0$ intuitívne algoritmicky vypočítateľných čiastočne funkcií. Existuje presne $\aleph_0$ intuitívne algoritmickt vypočítateľných totálnych funkcií.*

Dôkaz. a) $\lambda \quad (0), \lambda \quad (1), \ldots, \aleph_0$ totálnych.

b) je maximálne $\aleph_0$ programov a teda vypočítateľných čiastočne je najviac $\aleph_0$. A navyše totálne sú podmnožinou čiastočných.

2 Teória vypočítateľnosti – poznámky z prednášky #2

Veta 2.0.2 *Existujujú nevypočítateľné funkcie.*

Dôkaz. Ak je vypočítateľná, tak existuje program, programov je spočítateľne veľa, ale funkcii jednej premennej z N do $\{0, 1\}$ je nespočitateľne veľa.

Veta 2.0.3 *Každá intuitívne algoritmicky vypočítateľná vypočítateľná čiastočne funkcia má* $\aleph_0$ *programov.*

Dôkaz. Mám funkciu, pridám $x = x + 1, x = x - 1$

Veta 2.0.4 *Neexistuje totálne algoritmicky vypočítateľná funkcia* g*, aby pre všetky* x, y*:* $g(x, y) = 0$ *AK* $\phi_x(y)$ *nie je definovaná, a* 1 *ináč.*

Dôkaz. Sporom: Diagonalizácia – $g(x, y)$ - univerzálne rozhodovacia pre pre naše algoritmy. $\Psi(x) = 1$ ak $g(x, x) = 0$ ($\phi_x(x)$ nie je definovaná) a je nedefinovaná ak $g(x, x) = 1$ ($\phi_x(x)$ je definovaná). $\Psi(x)$ má svoje číslo, $\Psi(x) = \phi_a(x)$. Zoberiem $\phi_a(z) = \Psi(a)$ je definovaná, práve vtedy ak $g(a, a) = 0$ ale to práve vtedy keď $\phi_a(a)$ nie je definovaná.

2.1 Vypočítateľné funcie, rekurzívne množiny a rekurzívne očíslovateľné množiny.

Definícia. Funkcia $f : N^k \to N$ sa nazýva vypo4ítateľnou, ak existuje algoritmus $\mathcal{A}$, ktorý ju vypočíta v nasledovnom zmysle:

- ak je hodnota $f(x_1, \ldots, x_k)$ definovaná pre $x_i \in N$, potom sa algoritmus $\mathcal{A}$ zastaví na vstupe $x_1, \ldots, x_k$ a vytlačí $f(x_1, \ldots, x_k)$.
- Ak je hodnota $f(x_1, \ldots, x_k)$ nedefinovaná pre $x_1, \ldots, x_k$, potom sa algoritmum nezastaví na vstupe $x_1, \ldots, x_k$.

Príklad. $Sg(x) =$ if $x = 0$ then 0 else 1
$\bar{S}g(x) =$ if $x = 0$ then 0 else 1
$\bar{S}g(x) = 1 - Sg(x)$

Poznámka. $f(x_1, \ldots, x_k)$ nie je definovaná, práve vtedy keď algoritmus A sa zacyklí alebo zastane a nič nedá na výstup.

Definícia. Množina $M \subseteq \mathbb{N}^k$ je rekurzívne vypočítateľná, ak jej charakteristická funkcia $\chi_M(x_1, \ldots, x_k)$ je vypočítateľná.

Príklad. $\chi_M(x_1, \ldots, x_k) = 1$ ak $x_1, \ldots, x_k \in M$, a 0 ináč.

Príklad. $\mathbb{N}$, if $n \in \emptyset$ then 1 else 0. – sú rekurzívne

2

Príklad. Existuje nerekurzívna množina $M \subset \mathbb{N}$.

Veta 2.1.1 *Každá konečná množina* $M \subseteq \mathbb{N}^k$ *je rekurzívna (algoritmicky). Nech* $M_1, M_2 \subseteq \mathbb{N}^k$ *a* M_1, M_2 *sú rekurzívne. Potom* $M_1 \cap M_2, M_1 \cup M_2$ *a* $M_1 \backslash M_2$ *sú rekurzívne.*

Dôkaz. a.) if $x = x_1$ alebo ... alebo $x = x_1$ then 1 else 0

b.) $\chi_{M_1}(x)$
$\chi_{M_2}(x)$
$\chi_{M_1 \cap M_2}(x) = \chi_{M_1}(x) \cdot \chi_{M_2}(x)$
$\chi_{M_1 \cup M_2}(x) = sg(\chi_{M_1}(x) + \chi_{M_2}(x))$
$\chi_{M_1 \backslash M_2}(x) = \chi_{M_1}(x) \cdot (1 - \chi_{M_2}(x))$

Cvičenie. Teraz sme predpokladali – pravda = 1, lož =0. Ako to bude, ak to vymeníme?

Veta 2.1.2 *Nekonečná množnina $M \subseteq \mathbb{N}$ je rekurzívna práve vtedy, keď je množinou hodnôt totálnej rastúcej vypočítateľnej funkcie.*

Dôkaz.

- $\Rightarrow$. Nech nekonečná $M \subseteq \mathbb{N}$ je rekurzívna. $\chi_M(x) = 1$ ak $x \in M$ a 0 ináč. Treba vytvoriť $f(x)$. $x_0 < x_1 < x_2 < \cdots < x_n < \cdots$ nekonečná rastúca postupnosť prvkov z M. $f(n) = x_n$

  $f(n)$ má program.

```
1) p:=0
2) x:=0
3) if χ_M(x)=1 then p:=p+1
4) while p<n+1 do
5)     x:=x+1;
6)     if χ_M(x)=1 then p=p+1
```

  Invariant riadok 3: x je posledné preverené číslo, p je počet kladných odpovedí medzi doteraz preverenými číslami. Na konci: $p = n + 1$ a invariant: $x = f(n + 1)$.

- $\Leftarrow$ Máme totálnu rastúcu vypočítateľnú funkciu $f : \mathbb{N} \to \mathbb{N}$. Vieme, že $Val(f) = M$.
  $x \in M$ ak $\exists n : x = f(n)$
  $x \notin M$ ak $\exists n : f(n) < x < f(n + 1)$ Netreba hľadať ďalej ako nejaké číslo. Aké?

Definícia. Množina $M \subseteq \mathbb{N}^K$ je rekurzívne očíslovateľná (alebo rekurzívne spočítateľná – recursive enumerable). Ak existuje generujúci algoritmus, ktorý postupne tlačí všetky prvky množiny M a žiadne iné.

Poznámka. Generujúci algoritmus – vlastnosti:

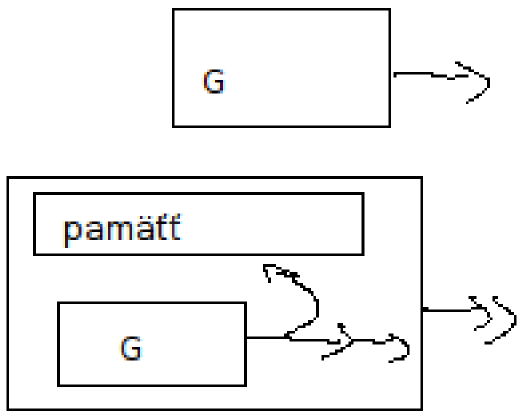
- Nemá vstup, má len začiatok, nemá koniec práce.
- Každý prvok sa vytlačí za konečný čas.
- čas medzi dvoma výpismi je konečný, ale nemusí byť konštantný.
- Poradie vypísaných prvok nie je rozhodujúce.
- Tlač toho istého prvku sa môže zopakovať.
- Od istého momentu sa už nič nemusí vypísať.

Príklad. Množina dvojíc $(n, n^2), n \in \mathbb{N}$ a n je nepárne je rekurzívne očíslovateľná.

```
x:=0;
while true do
    if (x mod 2=1) then write((x,xˆ2))
    x:=x+1
```

Ako odstrániť generovanie duplikátov?

.



Veta 2.1.3 *Nech $M \subseteq \mathbb{N}$. Potom nasledovné tvrdenia sú ekvivalentné.*

a) M je rekurzívne očíslovateľné.

b) M je definičným oborom (nejakej) vypočítateľnej funkcie. t.j. $(\exists f)(M = Arg(f))$

c) M je oblasťou hodnôť vypočítateľnej funkcie. t.j. $(\exists f)(M = Val(f))$

d) $c\chi_M$ je vypočítateľná funkcia.

Dôkaz.
- Nech M je rekurzívne vyčísliteľná. Existuje generujúci algoritmus, ktorý generuje $a_0, a_1, \ldots, a_n, \ldots$. Ak $f(x)$ je definovaný, x je generované, ak $f(x)$ nie je definované, x nie je generované. Nech $f(x) =^{def} 1$ ak x je generované a ináč je to nedefinované. – je to vypočítateľná funkcia (čakám na x. Ak bude generovaný, vypočítam, ak nie – cyklus – nedefinovaná). Zároveň $f(x)$ je $c\chi_M$. Dokázali sme, že z a) vyplýva b) aj d).

- Nech $g(x) =^{def} x$ ak x je generované, alebo je to nedefinované, ak x nie je generované. Je to vypočítateľná funkcia a dokázali sme že z a) vyplýva c).

- Nech f je vypočítateľná funkcia algoritmom B. Spustíme algoritmus pre všetky prirodzené čísla.

$B(0)$	$B(1)$	$B(2)$	$\ldots$	$B(n)$
k_{00}	k_{10}	k_{20}		
k_{01}	k_{11}			
k_{02}				
$\ldots$				
				k_{np}

  Pôjdeme po diagonálach (také, aby sme prešli každý krok) – generujeme vstup $M = Arg(f)$ čiže z b) aj d) vyplýva a. Tiež vieme generovať výstupnú hodnotu, čím sme dostali že $M = Val(f)$ a tým sme splnili, že z c) vyplýva a).

Poznámka. V prípade, že $M \subseteq \mathbb{N}^K$, potom c) musíme vyhodiť, ale a), b), d) sú ekvivalentné.

Veta 2.1.4 *Nech $M \subseteq \mathbb{N}$. Množina M je rekurzívne očíslovateľná $\Leftrightarrow$ $M = \emptyset$ alebo M je oblasťou hodnôt totálne vypočítateľnej funkcie.*

Dôkaz. Nech M je rekurzívne očíslovateľná a neprázdna.

$\Leftarrow$ Necháme bežať generátor. V každom takte "generátora" zvýšime n, a $f_M(n) = x$, kde x je posledné vypísané číslo z generátora. – je to vypočítateľná funkcia.

- ⇒ Nech máme funkciu, ktorá je totálna a vypočítateľná. Generujeme – najskôr generujeme $f(0)$, potom $f(1)$, potom $f(2)$,....

  Algoritmus:

```
i:=0
while true do
    write(f(i))
    i:=i+1
```

Veta 2.1.5 *Zjednotenie, prienik rekurzívne očíslovateľných množín je rekurzívne očíslovateľná.*

Dôkaz.

1. Zjednotenie: Chvíľku generujeme v jednom, chvíľku generuje v druhom a čo vypadne z ktoréhokoľvek, to vypíšem.
2. Prienik: Chvíľku generujeme v jednom, chvíľku v druhom, to, čo vyplujú si zapamätáme, a ak raz sa stane, že boli oba vypľuté, tak to vypľujem. Skrátka treba pamäť.

Poznámka. Pre rozdiel to už neplatí.

Veta 2.1.6 $L \subset \mathbb{N}, K \subset \mathbb{N}$ *sú rekurzívne očíslovateľné, potom* $L \times K \subset \mathbb{N} \times \mathbb{N}$ *je rekurzívne očíslovateľná.*

Dôkaz. Generujem paralelne, pamätám si, vždy keď príde nový, vypíšem dvojice, ktoré s ním viem vytvoriť.

Veta 2.1.7

a) Každá rekurzívna množina je rekurzívne očíslovateľná.

b) Postova veta: Ak množina $M \subseteq \mathbb{N}$ *ako aj jej doplnok je rekurzívne očíslovateľný, potom* M *je rekurzívna.*

Dôkaz.

a)
```
x:=0
while true do
    if χ_M(x) then
        write(x)
    x;=x+1;
```

b) Paralelne skúšame, či tam patrí tam alebo do doplnku, časom dostaneme výsledok z jedného a teda vieme výsledok vždy.

Veta 2.1.8 *Množina* $M \subseteq \mathbb{N}$ *je rekurzívne spočítateľná* $\Leftrightarrow$ M *je projekciou nejakej rekurzívnej množiny* $Q \subseteq \mathbb{N} \times \mathbb{N}$, *t.j.* $x \in M \Leftrightarrow (\exists y)((x, y) \in Q)$

Dôkaz. Na domácu úlohu, nabudúce zborovo zaspievať.

3 Teória vypočítateľnosti – poznámky z prednášky #3

Veta 3.0.9 *Množina $M \subseteq \mathbb{N}$ je rekurzívne spočítateľná $\Leftrightarrow$ M je projekciou nejakej rekurzívnej množiny $Q \subseteq \mathbb{N} \times \mathbb{N}$, t.j. $x \in M \Leftrightarrow (\exists y)((x, y) \in Q)$*

Dôkaz.

$\Leftarrow$ Nech Q je rekurzívna $\Rightarrow$ je rekurzívne očíslovateľná $\Rightarrow$ (lebo projekcia rek. očíslovateľnej množiny je rekurzívne očíslovateľná – vynechaním nepotrebných súradníc) M je rekurzívne spočítateľná.

$\Rightarrow$ Nech M je rekurzívne spočítateľná. To znamená, že existuje generátor, ktorý M generuje. Spravím dvojice $(x, k), x \in M$ k je počet krokov za ktoré sa x vygeneruje. To je rekurzívne očíslovateľná množina Q.

3.1 Rekurzívna očíslovateľnosť a vypočítateľnosť

Veta 3.1.1 *Funkcia $f : \mathbb{N} \to \mathbb{N}$ je vypočítateľná vtedy a len vtedy, keď jej graf $f = \{(x, y)|f(x)$ je definované a $f(x) = y\} \subseteq \mathbb{N} \times \mathbb{N}$ je rekurzívne očíslovateľná množina.*

Dôkaz.

$\Rightarrow$ Nech $f : \mathbb{N} \to \mathbb{N}$ je vypočítateľná (existuje algoritmus, čo počíta f). Diagonálne paralelne pustíme naraz všetky algoritmy, ktoré skončia, tie vypisujem.

$\Leftarrow$ Generujem a čakám na x.

Cvičenie. Rozšíriť na k-tice.

Definícia. Nech $f : \mathbb{N} \to \mathbb{N}$ je čiastočná funkcia a nech $A \subseteq \mathbb{N}, B \subseteq \mathbb{N}$. Potom $f(A) = \{y|(\exists x)x \in A \wedge (x, y) \in f)\}$ (obraz). $f^{-1}(B) = \{x|(\exists y)y \in B \wedge (x, y \in f\}$ (vzor).

Veta 3.1.2 *Nech $f : \mathbb{N} \to \mathbb{N}$ je vypočítateľná funkcia. A nech $A \subseteq \mathbb{N}, B \subseteq \mathbb{N}$ sú rekurzívne očíslovateľné množiny. Potom aj obraz $f(A)$ a vzor $f^{-1}(B)$ sú rekurzívne očíslovateľné.*

Dôkaz. f je vypočítateľná – vieme jej graf generovať. Zoberieme generátor A a generátor grafu. Naraz pustíme oba generátory a zapamätávame si výsledky, a keď nájdeme match, tak to hodíme na výstup. Podobne to funguje aj s generátorom B...

Poznámka. (graf f) $\cap (\mathbb{N} \times B) \to^{projekcia} = f^{-1}(B)$ (graf f) $\cap (A \times \mathbb{N}) \to^{projekcia} = f(A)$

Cvičenie. Nech $F \subseteq \mathbb{N} \times \mathbb{N}$ je rekurzívne očíslovateľná množina (neprázdna). Ukážte, že existuje vypočítateľná funkcia $f : \mathbb{N} \to \mathbb{N}$ taká, že $f \subseteq F$ (s maximálnym definičným oborom)

Riešenie.

a) $f = \emptyset$ – nikde nie je definovaná (ale už so zmeneným zadaním je toto zle:-).

b) Máme generátor G množiny F. Ak vygeneruje (x, y), tak sa pozrem, či už som x vygeneroval, ak nie, tak vyhodím (x, y), a ináč si zapíšem x.

Cvičenie. Nech $M \subseteq \mathbb{N}$ je nekonečná, rekurzívne očíslovateľná množina. Ukážte, že existuje nekonečne veľa poradí, generovania M, takých, že pre ne existuje generátor.

Riešenie. Každý generátor bude mať parameter p. Generátor M_p funguje ako generátor (bez opakovania) množiny M, ale ak vypočíta p-ty výsledok, počká aj na $p+1$ výsledok a v poradí ich vymení. Alebo najskôr vypočíta prvých p a potom ich dá v opačnom poradí. Alebo dá p-ty ako prvý, prvý ako p-ty.

Cvičenie. Nech $M \subseteq \mathbb{N}, K \subseteq \mathbb{N}$ sú rekurzívne očíslovateľné s neprázdnym prienikom. Ukážte, že existujú podmnožiny $M' \subseteq M, K' \subseteq K$, ktoré sú rekurzívne očíslovateľné, ale $M' \cap K' = \emptyset$, ale $M' \cup K' = M \cup K$.

Riešenie. Generujeme M aj K. Ak príde skôr z M, tak ho vygeneruje M', ináč ho vygeneruje K'.

Cvičenie. Ukážte, že každá rekurzívne očíslovateľná množina M sa dá zapísať v tvare očíslovanej postupnosti, pričom $f(0), f(1)$, pričom f je vypočítateľná a bez opakovania.

Riešenie. Máme generátor M, generujeme, vyhadzujeme duplikáty a pridávame poradie. Toto je vypočítateľné: dostaneme (x, y) a počkáme prvých x rôznych.

Cvičenie. Každá nekonečná rekurzívna očíslovateľná množina $M \subseteq \mathbb{N}$ obsahuje nekonečnú rekurzívnu podmnožinu.

Riešenie. M je nekonečná postupnosť – M obsahuje nekonečnú rastúcu podpostupnosť. Pamätáme si posledné maximum a ak príde väčší, tak ho vyhodíme. Je to rekurzívne – ak je maximum už väčšie ako vstup, tak viem, že ho už nevygenerujem.

Cvičenie. Ku každej vypočítateľnej funkcii jednej premennej existuje vypočítateľná funkcia g, ktorá (je "pseudoinverzia") spĺňa vlastnosti:

a) definičný obor g=obor hodnôt f

b) $f(g(f(x))) = f(x)$ pre všetky x z definičného oboru f.

Riešenie. Zoberiem (x, y) vyhodím (y, x), ale ak už také y bolo, tak nevyhodím.

3.2 Univerzálne funkcie a nerekurzívne množiny

Problém algoritmicky je algoritmicky rozhodnuteľný – je rekurzívna množina, nie je rozhodnuteľný – nie je rekurzívna množina.

Definícia. Budeme hovoriť, že funkcia dvoch premenných $U : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ je univerzálnou funkciou pre triedu T funkcii jednej premennej $(f : \mathbb{N} \to \mathbb{N})$ ak

a) Pre každé prirodzené číslo funkcia $U_n : x \to U(n, x)$ patrí do T.

b) Pre každé $f \in T$ existuje n také, že pre všetky $x \in \mathbb{N}$ bude $f(x) = U_n(x) = U(n, x)$

Poznámka. Ak T má univerzálnu funkciu, tak $|T| \leq \aleph_0$.

Poznámka. Ak $f(x) = U(n, x)$, tak n sa volá číslo funkcie f.

Poznámka. Funkcia z T môže mať viacej (aj nekonečne veľa) čísiel.

Cvičenie. Toto cvičenie nebolo dosť dobré na to, aby sa dostalo do týchto poznámok`:-P`

Cvičenie. Zadefinujte univerzálnu funckciu pre triedu funkcií $f : \mathbb{N}^k \to \mathbb{N}$.

Veta 3.2.1 *Existuje vypočítateľná funkcia dvoch premenných, ktorá je univerzálnou funkciou pre triedu vypočítateľných funkcii jednej premennej.*

Dôkaz. O texte $z \in \Sigma^*$ vieme rozhodnúť, či je to výpočet, alebo nie. Potom z nazývame program. Navyše vieme algoritmicky rozhodnúť, či počíta funkciu jednej premennej. Teda máme generátor programov. Máme programy $p_0, p_1, \ldots$. Iné funkcie vypočítateľné nie sú (nemáme na nich program).

$U(n, x)$ počítame nasledovne – vygenerujem program s číslom n, čiže p_n. Do neho dosadím číslo x. Ak dá výsledok, mám hodnotu, ináč je to nedefinované. U môže byť aj čiastočná funkcia.

Definícia. Budeme hovoriť, že množina $W \subseteq \mathbb{N} \times \mathbb{N}$ je univerzálnou množinou pre triedu množín P prodmnožín prirodzených čísiel, ak

a) Pre každé $n \in N$ existuje množina $W_n = \{x|(n,x) \in W\} \in P$

b) iných množín v P niet: $(\forall M \in P)(\exists n \in \mathbb{N}) M = W_n$

Veta 3.2.2 *Existuje rekurzívne očíslovateľná množina dvojíc prirodzených čísiel, ktorá je univerzálna pre triedu všetkých rekurzívne očíslovateľných množín prirodzených čísiel.*

Dôkaz. M je rekurzívne očíslovateľná – má generátor. M je definičným oborom vypočítateľnej funkcie. Je tiež oborom hodnôt vypočítateľnej funkcie. Tiež $x \in M \Leftrightarrow (\exists y)(x,y) \in Q$

$D(f_i) = M_i \ f_i$

$(n,x) \in W \Leftrightarrow U(n,x)$ je definovaná.

Je generovateľná – diagonálne.

Cvičenie. Existuje rekurzívna množina $R \subseteq \mathbb{N} \times \mathbb{N}$, ktorá je univerzálna pre triedu všetkých rekurzívnych podmnožín $\mathbb{N}$?

Riešenie. Nech existuje. M je rekurzívna, ak jej χ_M je vypočítateľná. Rekurzívnych množín je nekonečne veľa.

	0	1	2	3	4
χ_{M_0}	0	1	1	1	0
χ_{M_1}	0	1	1	1	0
...					
χ_{M_i}	0	1	1	1	0

Zoberiem diagonálu, tam to znegujem $\chi(x) = 1 - \chi_x(x)$ Táto tam nepatrí, ale je rekurzívne spočítateľná.

3.3 Diagonálne konštrukcie

Veta 3.3.1 *Neexistuje totálna vypočítateľná funkcia dvoch premenných, ktorá je univerzálna pre triedu všetkých totálnych vypočítateľných funkcii jednej premennej.*

Dôkaz. Diagonalizácia.

Zoberieme všetky totálne vypočítateľné, zoradíme $(f_1, f_2, \dots)$, spravíme totálnu vypočítateľnú, ktorá tam nie ju $U(x,x) + 1$ – nie je rovná žiadnej f_i.

4 Teória vypočítateľnosti – poznámky z prednášky #4

Prišiel som nekkoro, začiatok je len odpísaný z tabule.

Veta 4.0.2 *Existuje vypočítateľná funkcia* $d : \mathbb{N} \to \mathbb{N}$*, pre ktrorú platí: Pre každú vypočítateľnú funkciu* $f : \mathbb{N} \to \mathbb{N}$ *existuje číslo* n *také, že platí* $f(n) = d(n)$*.*

Dôkaz. $d(n) = U(n, n)$.

Veta 4.0.3 *Existuje vpočítateľná funkcia* $f : \mathbb{N} \to \mathbb{N}$*, ktorá nemá vypočítateľné zúplnenie na* $\mathbb{N}$*.*

Dôkaz. Nech $f'(n)$ je vypočítateľné zúplnenie funkcie $f(n)$, potom $\exists n : f'(n) = d(n) = U(n, n)$.
$f;(n) = d(n)$.
$U(n, n) + 1 \neq U(n, n), U(n, n)$ je definovaná.
definovaná $\neq$ nedefinovaná $U(n, n)$ nie je definovaná.

Cvičenie. Ukážte, že ani $U(n, n)$ nemá vypočítateľné zúplnenenie.

Riešenie. Ak $U(n, n)$ nie je vypočítateľné zúplnenie, potom $U(n, n) + 1$ nie je vypočítateľné zuplnenie.

Veta 4.0.4 *Existuje rekurzívne očíslovateľná množina, ktorá nie je rekurzívna.*

Dôkaz. Nech $f(x)$ je vypočítateľná funkcia, ktorá nemá vypočítateľné zúplnenie. F - definičný obor f ($Arg(f) \neq \mathbb{N}$) F je rekurzívne očíslovateľná množina (je to definičný obor vypočítateľnej funkcie). F nie je rekurzívna množina.

Nech F je rekurzívna. Ak $x \in F$, tak vyhodím $f(x)$, ináč vyhodím 0, čo je vypočítateľné zúplnenie f, čo je spor.

Poznámka. Funkcia $d(n) = U(n, n)$ nemá vypočítateľné zúplnenie. Preto jej definičný obor je množina, ktorá je rekurzívne očíslovateľná, ale nie je rekurzívna. Podľa Postovej vety, to znamená, že doplnok k jej definičnému oboru nie je rekurzívne očíslovateľný (komplement $Arg(U(n, n))$ nie je rekurzívne očíslovateľný). Z toho vyplýva, že definičný obor celej U je rekurzívne očíslovateľný. Z toho vyplýva, že doplnok k $Arg(U(n, x))$ nie je rekurzívne očíslovateľný.

Problém zastavenia turingovho stroja nie je algoritmicky riešiteľný.

Priamy ťah na bránku: Máme formalizáciu pojmu algoritmus. Prvá podmienka je, že chceme vedieť o texte rozhodnúť, či daný text opisuje program, alebo nie. Chceme číslovanie programov $(p_0, p_1, \dots)$, číslovanie funkcií $\mathbb{N} \to \mathbb{N}$, univerzálnu funkciu $U(n, x)$, diagonála $U(n, n)$ nemá vypočítateľné zúplnenie. A teda $Arg(U(n, n))$ je rekurzívne očíslovateľná množina, ktorá nie je rekurzívna množina.

Definícia. Budeme hovoriť, že množina je imúnna, ak je nekonečná a neobsahuje nekonečné rekurzívne očíslovateľné podmnožiny (Rekurzívne očíslovateľná množina sa nazýva prostou, ak jej doplnok je imúnny).

Poznámka. Prostá funkcia nemôže byť rekurzívna (Postova veta).

Veta 4.0.5 *Existuje prostá množina.*

Dôkaz. Potrebujeme zostrojiť $S \subseteq \mathbb{N}$ a jej doplnok $\bar{S}$.
S je rekurzívne očíslovateľná.
$\bar{S}$ je imúnna množina – je nekonečná, neobsahuje rekurzívne očíslovateľné podmnožiny.

Stačí: do S dáme aspoň jeden prvok z každej nekonečnej rekurzívne očíslovateľnej množiny ale tak, aby mimo S ostalo nekonečne veľa prvkov. Napríklad: Z množiny číslo i vyberieme prvok s veľkosťou aspoň $2i$.

W – univerzálna množina?

Nech $T = \{(i, x) | (x \in w_i) \wedge (x > 2i)\} = W \cap \{(i, x) | (x > 2i)\}$

W – rekurzívne očíslovateľná množina, $\{(i,x)|(x > 2i)\}i$ je rekurzívna množina – aj očíslovateľná, čiže prienik je tiež rekurzívne očíslovateľná množina.

Pri generovaní monžiny T budeme odhadzovať tie dvojice (i,x), ktorého prvý člen i sme už „stretli". Z každého w_i spravíme jedno číslo (ak w_i je nekonečné).

Takto vygenerujeme množinu T'. S je projekcia množiny T'.

S je rekurzívne očíslovateľná množina, má spoločný prvok s každou nekonečnou rekurzívne očíslovateľnou množinou a $\bar{S}$ je nekonečná množina, lebo z prvých i množín sme vybrali maximálne i prvkov a aspoň i prvkov ostalo.

Veta 4.0.6 *Existuje vypočítateľná funkcia $d_2 : \mathbb{N} \to \{0,1\}$ ktorá nemá vypočítateľné zúplnenie na množine vstuov na $\mathbb{N}$.*

Dôkaz. $d_2(x) = \bar{sg}(U(x,x)) = 1$ ak $U(x,x) = 0$, ak $U(x,x) > 0$ je to 0 a ak je to nedefinované, tak je to nedefinované.

Definícia. Dve disjunktné množiny X, Y sú oddeliteľné množinou C ak $X \subseteq C$ a $C \cap Y = \emptyset$.

Veta 4.0.7 *Existujú dve disjunktné rekurzívne očíslovateľné množiny, ktoré nie sú oddeliteľné žiadnou rekurzívnou množinou.*

Dôkaz. Nech $X = \{x|d_2(x) = 1)\}$ a $Y = \{x|d_2(x) = 0\}$. Obidve sú rekurzívne očíoslovateľné. Nech $x \subseteq C$, $d_2(x) = 1$ nemení hodnotu, $C \cap T = \emptyset$ $d_2(x) = 0$ nemení hodnotu. Potom $\chi_C(s) = 1$ ak $x \in C$ a 0 ak $x \notin C$. Je to zúplnenie $d_w(x)$ a to nemôže byť vypočítateľné. Z toho vyplýva, že C nie je rekurzívne.

4.1 Primitívne rekurzívne funkcie

Primitívne rekurzívne funkcie $\subset$ všeobecné rekurzívne funkcie $\subset$ čiastočne rekurzívne funkcie.

Máme k dispozícii:

- $0 = \lambda(0)$
- $\delta(x) = \lambda x(x+1)$
- $I_i^n(x_1, \ldots, x_i, \ldots, x_n) = x + i$ - $\lambda x_1, \ldots, x_n(x_i)$.
- primitívna rekurzia (for cyklus – parameter, koľko krát sa cyklus opakuje)
- regulárna substitúcia – strom – potiaľto sú primitívne rekurzívne.
- minimalizácia pre y $(f(y, x_1, \ldots, x_n) = 0)$ – lineárne prehľadávanie – odtiaľto sú čiastočne rekurzívne
- 0 je pravda, ostatné nie pravda.

Koniec úvodu.

Definícia. (Regulárna substitúcia/skladanie)

Nech f je n-árna (čiastočná) funkcia $(n > 0)$. Nech $g, f_1, \ldots, f_n$ sú už m-árne (čiastočné) funkcie. Budeme hovoriť, že (čiastočná) funkcia g vzniká skladaním (substitúciou) z (čiastočnúch) funkcii $f, f_1, \ldots, f_n$ a písať $g = \mathbb{S}(f, f_1, \ldots, f_n)$ ak pre všetky $x_1, \ldots, x_n$ platí, že $g(x_1, \ldots, x_n) = f(f_1(x_1, \ldots, x_m), \ldots, f_n(x_1, \ldots, x_m))$.

Poznámka. Odteraz funkcie môžu byť čiastočné a nebudeme to písať!.

Definícia. (Primitívna rekurzia)

Nech f je $(n+1)$-árna a g je $(n+2)$-árna a h je n-árna čiastočná funkcia na $\mathbb{N}$, kde $n \geq 0$. Hovoríme, že f vzniká z g, h operáciou primitívnej rekurzie, a píšeme že $f = R(g,h)$ ak pre všetky $x_1, \ldots, x_n, y \in \mathbb{N}$ platí:

1. $f(0, x_1, \dots, x_n) = h(x_1, \dots, x_n)$
2. $f(y+1, x_1, \dots, x_n) = g(y, f(y, x_1, \dots, x_n), x_1, \dots, x_n)$

Príklad. $f(y, x) = x^y$.
$f(0.x) = x^0 = 1 = \lambda x(1)$.
$f(y+1, x) = x^{y+1} = x^y \cdot x = g(y, x^y, x) = \lambda\alpha, \beta, \gamma(\beta \cdot \gamma)$.
$\lambda x, y(x^y) = R(\lambda\alpha, \beta, \gamma(\beta \cdot \gamma), \lambda x(1))$.

Cvičenie. Ukážte, že ak g, h sú totálne, tak aj $R(g, h)$ je totálna funkcia.

Riešenie. Indukciu cez y. Prvý krok je očividný, lebo h je definovaná. Druhý krok – pre y je to definované, mám definované vstupy a g je totálne, tak mám aj definovaný výstup, takže je to totálne.

Cvičenie. $f(0) = 1$
$f(n) = \uparrow$ ak $n \geq 1$ – nie je definovaná. Napíš ju ako primitívnu rekurziu dvoch funkcií.

Riešenie. $h = \lambda(1)$
$f(n+1) = g(n, f(n)) = \uparrow = \lambda\alpha, \beta(\uparrow)$

5 Teória vypočítateľnosti – poznámky z prednášky #5

1. Funkcie:
   $0 \ \lambda$
   $x+1 \ s(x) = \lambda x(x+1)$
   $I^n_M(x_1, \ldots, x_n) = x_m$

2. Operácie:
   $\mathcal{S}^{n+1}(f, f_1, \ldots, f_n)$ – skladanie – substitúcia
   $\mathcal{R}(g, h)$ – primitívna rekurzia.

Definícia. Budeme hovoriť, že funkcia f je primitívne rekurzívna, ak vzniká z funkcií 0, s, I^n_m konečným počtom operácii skladania $\mathcal{S}$ a primitívnej rekurzie $\mathcal{R}$, t.j ak existuje konečná postupnosť funkcii $f_1, \ldots, f_k$ taká, že $f = f_k$ a $\forall i \in \{1, \ldots, k\}$ platí jedna z nasledovných možností:

a) $f_i = 0$

b) $f_i = s$

c) $f_i = I^n_m$

d) $f_i = \mathcal{S}^{m+1}(f_j, f_{j_1}, \ldots, f_{j_m}) \quad 1 \leq j, j_1, \ldots, j_m < i$

e) $f_i = \mathcal{R}(f_a, f_b), a, b < i$

Poznámka. Primitívne rekurzívne funkcie vznikli okolo roku 1860. Okolo roku 1950 vznikol v matematike veľký ??? A museli to riešiť.

Veta 5.0.1 *Množina PRF primitívne rekurzívnych funkcii je najmenšia množina ($\subseteq$) obsahujúca funkcie $0, s, I^n_m$ a uzavretá na operácie $\mathcal{S}, \mathcal{R}$.*

Dôkaz. Sporom. Nech M obsahuje $0, s, I$ a je uzavretá na $\mathcal{S}, \mathcal{R}$. Nech $f \in PRF$, potom $f \in M$? Áno, lebo ak zoberieme postupnosť $f_1, \ldots, f_k$ a tá je dobrá aj v M. QED

Poznámka. Primitívne rekurzívne funkcie sú totálne.

Veta 5.0.2 *Funkcia, ktorá vznikla konečným počtom operácii skladania a primitívnej rekurzie z primitívne rekurzívnych funkcii je primitívne rekurzívna.*

Dôkaz. Dôkaz je trápny...

Veta 5.0.3 *Nech množina funkcii M obsahuje všetky I^n_m a je uzavretá na regulárnu substitúciu (skladanie). Nech funkcia $f(x_1, \ldots, x_m), m \neq 0$ patrí do M. Nech $K_1, \ldots, K_m$ je ľubovoľná postupnosť prvkov množiny $\{1, \ldots, n\}$. Potom aj funkcia $g(x_1, \ldots, x_n) = f(x_{K_1}, \ldots, x_{K_m}) \in M$.*

Dôkaz. $f = S^{m+1}(f, I^n_{K_1}, \ldots, I^n_{K_m})$.

Príklad. Nech $\lambda xy(x^y) \in M$
$\lambda x(x^x) \in M.$ – stotožnenie premenných.
$\lambda xyz(x^y) \in M.$ – dodanie fiktívnej premennej.
$\lambda xz(x^x) \in M.$
$\lambda x, y(y^n) \in M.$ – permutácia premenných.

Veta 5.0.4 *Všetky konštantné funkcie sú primitívne rekurzívne.*

Dôkaz. Je ľahký.

Veta 5.0.5 *Nech množina funkcii M obsahuje všetky I^n_m, všetky unárne konštanty K^1_a a je uzavretá na regulárnu substitúciu. Nech funkcia $f(x_1, \ldots, x_n)$, $n \neq 0$ patrí do M. Nech $a_1, \ldots, a_k \in \mathbb{N}, k < n$. Potom aj funkcia $g(x_k + 1, \ldots, x_n) = f(a_1, \ldots, a_k, x_{k+1}, \ldots, x_n)$ patrí do M.*

Dôkaz. $\mathcal{S}^{n+1}(f, \mathcal{S}^2(K_{a_1}, I^{n-k}_1), \ldots, \mathcal{S}^2(K_{a_k}, I^{n-k}_k), I^{n-k}_1, \ldots, I^{n-k}_{n-k})$

Poznámka. $k < n$, lebo argument funkcie musí byť aspoň jedna premenná. Čo ak chceme zapchať všetkých? Ako to bude vyzerať? Potom $f(a_1, \ldots, a_n) = K^0_{f(a_1,\ldots,a_n)}$.

Veta 5.0.6 *$\lambda xy(x + y), \lambda xy(x \cdot y), \lambda xy(x^y)$ sú primitívne rekurzívne funkcie.*

Dôkaz. Použijeme primitívnu rekurziu (a vždy predchádzajúcu funkciu).

- $x + y$:
  $x + 0 = x = I^1_1(x)$
  $x + (y + 1) = (x + y) + 1 = g(y, x + y, x) = I^3_2(y, x + y, x) + 1$
  $\lambda xy(x + y) = \mathcal{R}(s(I^3_2), I^1_1)$
- $x\dot{y}$:
- x^y:

Veta 5.0.7 *$\lambda xy(x \dot{-} 1)$ je primitívne rekurzívna.*

Dôkaz.

Veta 5.0.8 *$sg(x)$ je primitívne rekurzívna funkcia.*

Dôkaz.

Veta 5.0.9 *$\lambda xy(x \dot{-} y)$ je primitívne rekurzívna funkcia.*

Dôkaz. $x \dot{-} y = 0$ ak $x \leq y$ a $x - y$ ináč.
$x \dot{-} 0 = x$ $x \dot{-} (y + 1) = x \dot{-} y \dot{-} 1$.
$g(y, x \dot{-} y, x)$
$\mathcal{R}(I^3_2 \dot{-} 1, I^1_1)$
$\mathcal{R}(\mathcal{S}(\dot{-}_1, I^3_2), I^1_1)$

Veta 5.0.10 *$|x - y| = (x - y) + (y = x)$ je primitívne rekurzívna funkcia.*

Dôkaz. $\mathcal{S}^3(+, \dot{-}, S^3(\dot{-}, I^2_2, I^2_1))$

Poznámka.

1. $A = B \rightarrow sg(|A - B|) = 0$
2. $A \neq B \rightarrow sg(|A - B|) = 1$
3. $A \leq B \rightarrow sg(A \dot{-} B) = 0$
4. $A > B \rightarrow gs(A \dot{-} B) = 1$

Veta 5.0.11 *(Veta o IFnutí)*
Nech $f_1, \ldots, f_{s+1}, h_1, \ldots, h_s \in PRF^{(n)}$. Nech pre žiadne $x_1, \ldots, x_n \in \mathbb{N}^n$ sa žiadne dve z funkcii $h_1, \ldots, h_s$ nerovnajú súčasne nule. Potom funkcia f definovaná predpisom $f(x_1, \ldots, x_n) = f_1(x_1, \ldots, x_n)$ ak $h_1(x_1, \ldots, x_n) > 0$
$f(x_1, \ldots, x_n) = f_2(x_1, \ldots, x_n)$ ak $h_2(x_1, \ldots, x_n) > 0$
$\vdots$
$f(x_1, \ldots, x_n) = f_s(x_1, \ldots, x_n)$ ak $h_s(x_1, \ldots, x_n) > 0$
$f(x_1, \ldots, x_n) = f_{s+1}(x_1, \ldots, x_n)$ ináč
je PRF.

Dôkaz. $f(\overline{x}) = f_1(\overline{x}) = f_1(\overline{x})\dot{\overline{sg}}(h_1(\overline{x})) + \cdots + f_s(\overline{x})\dot{(}h_s(\overline{x})) + f(s + 1).sg(h1, h2, ...)$

6 Teória vypočítateľnosti – poznámky z prednášky #9

Definícia. Číslo konfigurácie $(q_i, a_0, a_0, \ldots, a_n)$ je číslo $2^i 3^{a_0} 5^{a_1} \ldots p_{n+2}^{a_n}$. Je to vždy väčšie ako 0.

Číslom konečnej postupnosti konfigurácii je číslo výpočtu $\alpha_0\alpha_1 \ldots \alpha_m$ je číslo $2^{num(\alpha_0)} 3^{num(\alpha_1) \ldots p_{m+1}^{num \alpha_m}}$.
Číslo inštrukcie:
$(q_i R_j P q_k) \ldots p_i^{2c(j,k)+1}$
$(q_i R_j M q_k) \ldots p_i^{2c(j,k)+2}$
$(q_i R_j q_m q_k) \ldots p_i^{2c^{(3)}(j,m,k)+3}$
Číslo konfigurácie:
$\alpha = (q_i, a_0, \ldots, a_j, \ldots, a_n)$ $x = 2^i 3^{a_0} \ldots \ldots p_{j+1}^{a_j} \ldots p_{n+2}^{a_n}$
$\beta = (q_k, b_0, \ldots, b_j, \ldots, b_n)$ $x = 2^i 3^{b_0} \ldots \ldots p_{j+1}^{b_j} \ldots p_{n+2}^{b_n}$
Číslo stroja:
$Z = p_0 p_1^{3c \ldots} \ldots$
Číslo postupnosti konfigurácii:
$y = 2^{num(\alpha_0)} \ldots p_t^{num(\alpha_t)} p_{t+1}^{num(\alpha_{t+1})} \ldots p_L^{num(\alpha_L)}$
$L = size(y)$
$size(A) = min\{y | \Sigma_{i=y+1}^{A} ex(i, A) = 0\} \leq A$

Definícia.
$M_{prech}(z, x, y)$ = konfigurácia číslo y vzniká z konfigurácie číslo x jediným krokom výpočtu stroja z.

(b) $M_{vyp}^{n+2}(y, z, x1, \ldots, x_n) = y$ je číslom výpočtu stroja z začínajúcim v konfigurácii $(q_1, 0x_1 \ldots x_n)$, pričom tento výpočet končí vnútorným stavom q_0, ktorý je nepredĺžiteľný.

(c) $m_{vyp}^{n} + 2(y, z, x_1, \ldots, x_n)$ - charakteristická funkcia predikátu $M_{vyp}^{n+2}(y-, z, x_1, \ldots . x+n)$.

(d) $m_{obs}(y)$ = obsah registra R_0 v poslednom člene konečnej postupnosti konfigurácii ktorá má číslo y.

Veta 6.0.12 *Nasledovný predikát je primitívne rekurzívny.*
$M_{prech}(z, x, y) = 0 < x \wedge 0 < y \wedge [(\exists i \leq z)(\exists j \leq z)(\exists k \leq z)$
$((ex(i, z) = 3c(j, k) + 1 \wedge ex(0, x) = i \wedge ex(0, y) = k \wedge ex(j + 1, x) + 1 = ex(j + 1, y) \wedge$
$(\forall t \leq x + y)(t \neq jarrowex(t + 1, x) = ex(t + 1, y)))$
$\vee\ (ex(i, z) = 3c(j, k) + 2 \wedge ex(0, x) = i \wedge ex(0, y) = k \wedge ex(j + 1, x) \dot{-} 1 = ex(j + 1, y) \wedge (\forall t \leq x + y)(t \neq jarrowex(t + 1, x) = ex(t + 1, y)))$
$\vee\ (\exists m \leq z)(ex(i, z) = 3c^{(3)}(j, m, k) + 3 \wedge ex(0, x) = i \wedge ex(0, y) = k \wedge ex(j + 1, x) = 0 \wedge (\forall t \leq x + y)(ex(t + 1, x) = ex(t + 1, y)))$
$\vee\ (\exists m \leq z)(ex(i, z) = 3c^{(3)}(j, k, m) + 3 \wedge ex(0, x) = i \wedge ex(0, y) = k \wedge ex(j + 1, x)! = 0 \wedge (\forall r \leq x + y)(ex(t + 1, x) = ex(t + 1, y))))]$

Dôkaz. Všetko čo sa použilo, je primitívne rekurzívne.

Veta 6.0.13 *Nasledovný predikát je primitívne rekurzívny.* $M_{vyp}^{n+2}(y, z, x_1, \ldots x_n) = ex(0, y) = 2^1 3^0 5^{x_1} \ldots p_{n+2}^{x_n} \wedge (\forall t \leq size(y) \dot{-} 1) M_{prech}(z, ex(t, y), ex(t + 1, y)) \wedge (ex(0, ex(size(y), y)) = 0) \wedge ex(0, z) = 0$

Dôkaz. Všetko, čo sa použilo, je primitívne rekurzívne.

Veta 6.0.14 *Nasledovná funkcia je primitívne rekurzívna:* $m_{obs} = ex(1, ex(size(y), y))$

Dôkaz. ...

Definícia. Budeme hovoriť, že funkcia $n + 1$ premenných $U : \mathbb{N}^{n+1} \to \mathbb{N}$ je univerzálnou funkciou pre triedu T funkcií n premenných, ak

a) pre každé $k \in \mathbb{N}$ funkcia $U_k : x_1, \ldots, x_n \to U(k, x_1, \ldots, x_n)$ patrí do T.

b) pre každú $f \in T$ sa nájde $k \in \mathbb{N}$ také, že pre všetky $x_1 \ldots x_n \in \mathbb{N}^n$ bude $f(x_1, \ldots, x_n) = U_k(x_1, \ldots, x_n) = U(k, x_1, \ldots, x_n)$. ($k$ nazývame číslom funkcie f).

Cvičenie. Nájdi univerzálnu funkciu pre triedu, ktorá obsahuje jednu funkciu.

Cvičenie. T má nekonečne veľa funkcií. Chceme univerzálnu funkciu, aby každá funkcia mala iba jedno číslo.

$f_i(x) = \lambda x(i)$. $U(k, x) = f_k(x)$.

Definícia. Pre každé číslo $n \in \mathbb{N}$ definujeme $n + 1$-árnu funkciu predpisom $\forall z, x_1, \ldots, x_n \in \mathbb{N}$. $m^{(n+1)}_{univ}(z, x_1, \ldots, x_n) = \phi^n_z(x_1, \ldots, x_n)$.

Veta 6.0.15 *Pre každé priorodzené číslo je čiastočná funkcia $m^{(n+1)}_{univ}(y, x_1, \ldots, x_n)$ univerzálna funkcia pre množinu všetkých n-árnych M-vypočítateľných (na Minského stroji) funkcii.*

Dôkaz. Každé $k \in \mathbb{N}$ je číslom nejakého stroja.

Veta 6.0.16 *Pre každé prirodzené číslo $\forall z, x_1, \ldots, x_n \in \mathbb{N}$ platí*

$$m^{(n+1)}_{univ}(z, x_1, \ldots, x_n) = m_{obs}(min(y, m^{(n+1)}_{vyp}(y, z, x_1, \ldots, x_n) = 0))$$

Dôkaz. Je opäť triviálny.

Veta 6.0.17 *Pre každé prirodzené $n \in \mathbb{N}$ je funkcia $m^{(n+1)}_{univ}$ je čiastočne rekurzívna univerzálna funkcia pre množinu $CRF^{(n)}$.*

Dôkaz. a) $m^{(n+1)}_{univ} \in CRF$

b) Univerzálnosť pre $CRF^{(n)}$. $f(x_1, \ldots, x_n) \in CRF^{(n)} \to f(x_1, \ldots, x_n)$ je M vypočítateľná $\to \exists$ stroj z: $f(x_1, \ldots, x_n) = \phi^n_z(x_1, \ldots, x_n)$.

Stroj z má číslo a a teda $f(x_1, \ldots, x_n) = m^{(n+1)}_{univ})(a, x_1, \ldots, x_n) = m_{obs}(min(y, m^{(n+2)}_{vyp}(y, a, x_1, \ldots, x_n) = 0))$;

Poznámka. $CRF^{(n)}$ = všetkým n-árnym funkciám vypočítateľným na minského stroji.

Veta 6.0.18 *VRF = totálne CRF*

Dôkaz. VRF - $0, +1, I, S, R$, regulárnou minimalizáciou (zachováva totálnosť)

Totálne CRF sú tie čiastočné, ktoré sú totálne.

$VRF \subseteq$ Totálne CRF

Totálne $CRF \subseteq VRF$

Nech $f \in$ totálne CRF. $F(x_1, \ldots, x_n) = m_{os}(min(y, m^{(n+2)}_{vyp}(y, a, x_1, \ldots, x_n) = 0))$. – máme tam PRF a aj totálnu, takže minimalizácia je regulárna.

Poznámka. V definícii by sa dalo požadovať, že môže byť iba jedna minimalizácia.

Veta 6.0.19 *(Kleene, o normálnej forme) Nech $n \in \mathbb{N}$. Potom existujú také primitívne rekurzívne funkcie $u \in PRF^{(1)}$ a $v \in PRF^{(n+2)}$, že každú n-árnu čiastočne rekurzívnu funkciu $f \in PRF^{(n)}$ môžeme zapísať v tvare $f(x_1, \ldots, x_n) = u(min(y, v(y, k, x_1, \ldots, x_n) = 0))$ pre nejaké $k \in \mathbb{N}$.*

Dôkaz. $u = m_{obs}, v = m_{vyp}$.

Téza 6.0.1 *(Churchova téza) Systém všetkých čiastočných(totálnych) algoritmicky vypočítateľných funkcii na prirodzených číslach je totožný so systémom všetkých čiastočne (všeobecne) rekurzívnych funkcii.*

6.1 Redukcia úloh (stupne nerozriešiteľnosti)

Definícia. (recursive many-to-one reduction) Nech $A, b \subseteq \mathbb{N}$ sú rekurzívne očíslovateľné (spočítateľné) množiny. Hovoríme, že množina A je m-redukovateľná (many-to-one) k množine B a píšeme $A \leq_m B \Leftrightarrow$ existuje všeobecne rekurzívna funkcia f taká, že pre všetky $x \in \mathbb{N}$ platí $x \in A \Leftrightarrow f(x) \in B$.

Množiny A, B sú m-ekvivalentné (píšeme $A =_m B$ – trojité rovná sa) vtedy a len vtedy, ak $A \leq_m B$ a $B \leq_m A$.

Veta 6.1.1 *Relácia $\leq_m$ je reflexívna a tranzitívna na $P(\mathbb{N})$. Relácia $=$ – trojité – je reláciou ekvivalencie na $P(\mathbb{N})$.*

Dôkaz. Trápne.

7 Teória vypočítateľnosti – poznámky z prednášky #10

Veta 7.0.2 *a)* $A \nsubseteq \mathbb{N} \Rightarrow \emptyset \leq_m A$

b) $\emptyset \neq A \subseteq \mathbb{N} \Rightarrow \mathbb{N} \leq_m A$

c) $\emptyset \nleq_m \mathbb{N}$ *a* $\mathbb{N} \nleq_m \emptyset$

d) $A =_m \emptyset \Rightarrow A = \emptyset$

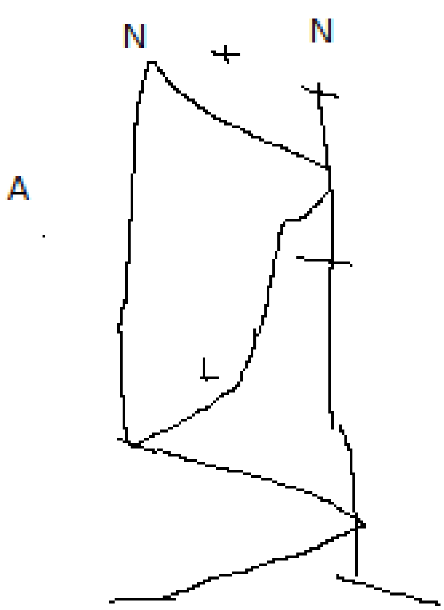
e) $A =_m \mathbb{N} \Rightarrow A = \mathbb{N}$

f) $\emptyset \nsubseteq A, B \nsubseteq$ *a* A, B *sú všeobecne rekurzívne množiny, potom* $A =_m B$

g) $A, B \subseteq \mathbb{N}, A \leq_m B$*,* B *je všeobecne rekurzívna množina, potom* A *je všeobecne rekurzívna množina.*

h) A *je všeobecne rekurzívna,* B *je rekurzívne očíslovateľná, ale nie je všeobecne rekurzívna, potom* $A \leq_m B, A \neq_m B$*.*

i) Všeobecne rekurzívne množiny tvoria 3 *triedy ekvivalencie*



Poznámka.

Dôkaz. a) Bude na písomke…

b)

c)

d)

e)

f)

g)

h)

i)

7.1 Rekurzívne očíslovateľné množiny

(tie, čo sa dajú generovať), definičný obor alebo obor hodnôť čiastočne definičných funkcii, projekcia všobecne rekurzívnej množiny

$VRM \subseteq ROM$

Definícia. Množina $A \subseteq \mathbb{N}$ je kreatívna (tvorivá), vtedy a len vtedy, ak A je rekurzívne očíslovateľná a $(\forall B)(B \in ROM \Rightarrow B \leq_m A)$

Veta 7.1.1 *Množina $K_R = \{c(y,x)|)y, x_\in Dom(m^2_{univ})\}$ je kreatívna. (Doména je Arg).*

Poznámka. $m^2_{univ}(y,x) = (\phi_y(x)$ je definovaná).

Dôkaz. a) K_R je rekurzívne očíslovateľná množ6ina, lebo je definičným oborom nejakej čiastočne rekurzívne funkcie. Ktorej? $g(z) = m^2_{univ}(L(z), R(z))$.

b) ukážeme $(\forall B)(V \in ROM \Rightarrow \leq_m K_R)$ To znamená, že i$c\chi_B(x) = 0$ ak $x \in B$ a je nedefinovaná ak $x \notin B$

$c\chi_B(x) = m^2_{univ}(b,x)$

$x \in B \Leftrightarrow c\chi_b(x) = 0 \Leftrightarrow m^2_{univ}(b,x) = 0 \Leftrightarrow (b,x) \in Dom(m^2_{univ}) \Leftrightarrow c(b,x) \in K_R$

i

Veta 7.1.2 *1. Kreatívna množina nie je všeobecne rekurzívna (jej doplnok, komplement, nie je generovatený).*

2. A je kreatívna, $B \in ROM$, , $A \leq_m B \Rightarrow B$ je kreatívny.

3. Ak A a B sú kreatívne, tak $A =_M B$.

4. kreatívne množiny tvoria triedu ekvivalencie.

Dôkaz.

1. Ak by kreatívna množina bola všeobecne rekurzívnou, potom podľa (g) sú všetky ROM všeobecne rekurzívne, čo je spor.
2. $\forall \alpha)(\alpha \leq_m A$ AA je kreatívna, a $A \leq_m B$, B je ROM, z tranzitívnosti vyplýva, že $(\forall \alpha)(\alpha \in ROM \Rightarrow \alpha \leq_m B)$
3. $A \leq_m B \wedge B \leq_M A$ a teda $A =_m B$
4. ...

Veta 7.1.3 $k_0 = \{y|y \in Dom(m^1_{univ})\}$.

Dôkaz. (Úpravou stroja $\Box Z$) $S(\Box Z, a) = R_1 := R_1 + a \rightarrow \Box Z$

$\Rightarrow \phi)\Box Z^1(a) = \phi^0_{S(\Box Z,a)}$

Zadefinujeme $g(0,a) = 0$, $g(y,a) =$ číslo stroja $S(\Box Z, a)$, y je číslo stroja $\Box Z$. Je to všeobecne rekurzívna funkcia.

Ukážeme, že $K_R \leq_m K_0$.

$z \in K_R \Leftrightarrow f(z) \in K_0$. $z = c(y,x)$.

$z \in K_R \Leftrightarrow \phi^1_y(a)$ je definovaná $\Rightarrow \phi^0_{g(y,a)}$ je definovaná $\Leftrightarrow g(y,a) \in K_0 \Leftrightarrow g(L(z), R(z)) \in K_0$.

Cvičenie. Nasledujúce množiny sú kreatívne:

a) $K_a = \{x|x \in Dom(m^2_{univ}(x,7))\}$. Množina všetkých čísiel M-strojov takých, že hodnota pre 7 je definovaná.

b) $K_b = \{x | m^2_{univ}(x, 7) = 5\}$

c) $K_c = \{c^3(z, y, x) | z = m^2_{univ}(y, x)\} \ldots \phi^1_y = z \Leftrightarrow (\phi^1_y(x)$ je definovaná $\wedge = z)$

Riešenie. a) (ukážeme, že $K_0 \leq_m K_a$).

$x \in K_0 \Leftrightarrow f(x) \in K_a$. „$f(x) = x$ také, že z R_1 odpočíta 7 (ale pod nulu neklesne)."

b) (spravíme $K_a \leq_m K_b$) – upravíme tak, že ešte skontrolujeme, či R_0 je 5.

c)

Písomka: a,b,c,d,e…., kreatívne mnoziny (korec, strana 51-52 - 6.48,6.49), strana 84,85 cvičenie 10.12

7.2 Aritmetická hierarchia

$W_e^{(k)} =^{def} Dom(\phi_e^{(k)}) = \{x_1, \ldots, x_k | \exists w T(e, x_1, \ldots, x_n, w) = 0\} \in ROM.$

Definícia. $K = \{x | x \in W_x\}$ – $\phi_x(x)$ je definovaná
$K_0 = \{c(x, v) | v \in W_x\}$ – $\phi_x(v)$ je definovaná

Veta 7.2.1 *Množiny K a K_0 sú rekurzívne očíslovateľné a nie sú všeobecne rekurzívne.*

Dôkaz. K, K_0 sú rekurzívne očíslovateľné, lebo sú doménou nejakej CRF.

a) K je $VRM \rightarrow \bar{K}$ je $VRM \rightarrow \bar{K}$ je ROM. Ukážeme že $\bar{K} \notin ROM$.

Nech $\bar{K}$ je rekurzívne očíslovateľná, potom má číslo, $(\exists e)\bar{K} = W_e$.

$\bar{K} = \{x | x \in W_x\} = W_e$.

Nech $e \in \bar{K} = W_e \Rightarrow e \in W_e \Rightarrow e \notin W_e$.

Nech $e \notin \bar{K} = W_e \Rightarrow e \notin W_e \Rightarrow e \in K \Rightarrow e \in W_e$. Spor – Russelov paradox.

A teda K nie je VRM

b) Redukciou. $x \in K \Leftarrow c(x, x) \in K_0 \Rightarrow c\chi_k(x) = 0 \Leftrightarrow_{K_0} (c(x, x)) = 0$.

Definícia. Nech $n \leq 1$. Hovoríme, že množina $A \subseteq \mathbb{N}^k$ je Σ_n-množina, ak existuje všeobecne rekurzívna relácia $R \subseteq \mathbb{N}^{k+n}$ taká, že $A = \{x_1, \ldots, x_k | (\exists v_1)(\forall v_2) \ldots (\substack{\exists \\ \forall} v_n) R(x_1, \ldots, x_k, v_1, \ldots, v_n)\}$

Hovoríme, že množina $A \subseteq \mathbb{N}^k$ je typu Π_n-množina, ak existuje všeobecne rekurzívna relácia $R \subseteq \mathbb{N}^{k+n}$ taká, že, $A = \{x_1, \ldots, x_k | (\forall v_1)(\exists v_2) \ldots (\substack{\forall \\ \exists} v_n) R(x_1, \ldots, x_k, v_1, \ldots, v_n)\}$

Príklad. $K = \{x | x \in W_x\} = \{x | \exists w T(x, x, w) = 0\} in \Sigma_1$.
$\bar{K} = \{x | x \in W_x\} = \{x | \forall w \not(T(x, x, w) = 0)\}$

Poznámka. $(\forall v_1)(\forall v_2)(\forall v_3) R(\bar{x}, v_1, v_2, v_3)$. $(\forall c(v_1, v_2, v_3)) R(\bar{x}, P_1(z), P_2(z), P_3(z))$.

Lema 7.2.2 *a) $ROM = \Sigma_1, VRM = \Sigma_1 \cap \Pi_1$*

b) $A \in \Sigma_n \Leftrightarrow \bar{A} \in \Pi_n; a \in \Pi_n \Leftrightarrow \bar{A} \in \Sigma_n$.

c) Zjednotenie a prienik k-árnych Σ_n množín (relácii) je opäť Σ_n (relácia) množina. Zjednotenie a prienik k-árnych Π_n množín(relácii) je opäť Π_n (relácia) množina.

d) Σ_n podmienky aj Π_n podmienky sú uzavreté na ohraničenú kvantifikáciu.

e) Σ_n podmienky sú uzavreté na existenčnú kvantifikáciu a Π_n podmienky sú uzavreté na všeobecnú kvantifikáciu.

f) $\Sigma_n \cup \Pi_n \subseteq \Sigma_{n+1} \cap \Pi_{n+1}$.

g) ak $A \leq_m B$ *a* $B \in \Sigma_n$*, potom aj* $A \in \Sigma_n$.

h) ak $A \leq_m B$ *a* $B \in \Pi_n$*, potom aj* $A \in \Pi_n$.

Dôkaz. a) $ROM = \Sigma_1$, lebo $A \in ROM \Leftrightarrow A = \{\bar{x} | (\exists v_1) g(\bar{x}, v) = 0\}$ g je VRF.
$VRM = \Sigma_1 \cap \Pi_1$ (Postova veta).

b) $A \in \Sigma_n \Leftrightarrow \bar{A} \in \Pi_n$.

c)

d)

e)

f)

g)

h)

8 Teória vypočítateľnosti – poznámky z prednášky #11

9 Teória vypočítateľnosti – poznámky z prednášky #12

Dôkaz. d) – vsetky pojdu jednym vrzomindukciou.

$(\exists v)P(\bar{x}, y, v)$ je Σ_n podmienka.

$(\exists u < z)(\exists v)P(\bar{x}, y, v) \Leftrightarrow (\exists v)(\exists y < z)P(\bar{x}, y, v)$

Ak $n = 1$ tak P je VR. potom to patrí Π_{n-1} pre $n \geq 2$.

$\frac{(\forall y<z)(\exists v)P(\bar{x},y,v)\Leftrightarrow(\exists w)(\forall y<x)(\exists v<w)P(}{x,y,v)}$

d)

d)

9.1 Aritmetická hierarchia

VRM $\subseteq \Sigma_1 \subseteq \Sigma_2 \subseteq \Sigma_3 \subseteq \cdots$
VRM $\subseteq \Pi_1 \subseteq \Pi_1 \subseteq \Pi_3 \subseteq \cdots$
$\Sigma_i \subseteq \Pi_{i+1}$
$\Pi_i \subseteq \Sigma_{i+1}$

Príklad. $Unb = \{x | W_x$ je nekonečná $\}$.

Riešenie. W_x je nekonečná $\Leftrightarrow (\forall v_1)(\exists v_2)(v_1 < v_2 \wedge v_2 \in W_x)$
Poznámka – $\Phi_x(v_2)$ je definovaná.
Platí: $\Sigma_1 = ROM$
$v_1 < v_2$ – primitívne rekurzívne.
$v_2 \in W_x$ – byť v definičnom obore, to nie je VRM, ale ROM
$min(y, T(e, x_1, \ldots, x_n, y)$ – ak $(\exists y)T(e, x_1, \ldots, x_n, y)$
T je PR
konjukcia – je ROM
Pridám existenčný kvantifikátor – je to uzavreté, stále ROM.
Pridáv všeobecný – je to potom Π_2

Príklad. $Rec = \{x | W_x$ je všeobecne rekurzívna $\}$

Dôkaz. W_x je rekurzívna $\Leftrightarrow (\exists y)(W_y = \bar{W_x}) \Leftrightarrow (\exists y)(\forall v)((v \in W_y \wedge v \notin W_x) \vee (v \notin W_y \wedge v \in W_x))$
$(v \in W_y)$ je ROM.
$(v \notin W_x)$ podľa (c),(f) $\Rightarrow$ je konjukcia v $\Sigma_2 \cap \Pi_w$. Druhý kus toho tam tiež patrí, $\vee$ to nezmení.
Všeobecný kvantifikátor to dá na Π_2 a existenčný na Σ_3.

Lema 9.1.1 *(Podozrenie o možnom kolapse hierarchie) Ak $\Sigma_n \subseteq Pi_n$ alebo $\Pi_n \subseteq \Sigma_n$. Potom pre každé $m \geq n$ platí vzťah $\Sigma_m = \Pi_m = \Sigma_n$.*

Dôkaz. a) Ukážeme $\Pi_n = \Sigma_n$. (z predpokladu, že $\Sigma_n \subseteq \Pi_n$, tak $\Pi_n \subseteq \Sigma_n$).

Ak $A \in \Pi_n$, potom $\bar{A} \in \Sigma_n$, potom $\bar{A} \in \Pi_n$, potom $A \in \Sigma_n$.

b) Ukážeme, že $\Sigma_{n+1} \subseteq \Sigma n$. $A = \{\bar{x} | (\exists v)P(\bar{x}, v)\}$.
$P(\bar{x}, v) \in \Pi_n = \Sigma_n$. Pridanie existenčného kvantifikátora to nezmení, bude stále v Σ_n.

c) $\Pi_{n+1} \subseteq Pi_n$.

d) – stačí spraviť indukciu – máme znenie lemy `:-)`

Poznámka. Ideme ukázať, že to neskolabuje.

Definícia. Množina $B \subseteq \mathbb{N}$ je Σ_n-kompletná ak $B \in \Sigma_n \wedge (\forall A)(A \in \Sigma_n \Rightarrow A \leq_m B)$.

Množina $B \subseteq \mathbb{N}$ je Π_n-kompletná ak $B \in \Pi_n \wedge (\forall A)(A \in \Pi_n \Rightarrow A \leq_m B)$.

Relácia $Q \subseteq \mathbb{N}^2$ je Σ_n-univerzálna ak $Q \in \Sigma_n$ a $(\forall A)(A \subseteq \mathbb{N} \wedge A \in \Sigma_n \Rightarrow (\exists a)(A = \{v|Q(a|v)\}))$

Relácia $Q \subseteq \mathbb{N}^2$ je Π_n-univerzálna ak $Q \in \Pi_n$ a $(\forall A)(A \subseteq \mathbb{N} \wedge A \in \Pi_n \Rightarrow (\exists a)(A = \{v|Q(a|v)\}))$

Definícia. $Q_1 = \{(x,v)|v \in W_x\} = \{(x,v)|\Phi_x(v)$ je definované $\}$.

$Q_{n+1} = \{(x,v)|(\exists y)(Q_n(x, c(v,y)))\}$

$H_n = \{c(x,v)|Q_n(x,v)\}$

$D_n = \{x|Q_n(x,x)\}$

Poznámka. $H_1 = K_0 = \{c(x,v)|v \in W_x\}$

$D_1 = K = \{x|x \in W_x\}$

Indukciou sa dá dokázať, že $Q_n \in \Sigma_n$.

Dokaz:

1. $Q_1 = \{(x,v)|v \in W_x\}$. Je to definičný obor nejakého algoritmu, $\Phi_x(v)$ je definovaná. – ROM – $= \{(x,v)|(\exists y)T(x,v,y)\}i$ – je to Σ_1
2. $Q_{n+1} = \{(x,v)|(\exists y)(T(x,v,y))\}$. Zoberieme to, znegujeme, kvantifikatory sa otocia, negacia sa otocia, a teda to patri do Σ_{n+1}. Preto aj $H_n \in \Sigma_n$ a $D_n \in \Sigma_n$.

Veta 9.1.2

1. *Každé Q_n je Σ_n-univerzálna a doplnok je Π_n-univerzálny.*
2. *H_n je Σ_n-kompletná, $\bar{H_n}$ je Π_n kompletná.*
3. *$D_n \in \Sigma_n \backslash \Pi_n$ a $\bar{D_n} \in \Pi_n \backslash \Sigma_n$.*

Veta 9.1.3 $(S-m-n)$

Pre každú dvojicu nenulových čísiel n a m existuje všeobecne rekurzívna funkcia $S_n^m \in VRF^{(n+1)}$ taká, že pre každé $e, x_1, \ldots, x_n$ platí:

$$\Phi^{(m)}_{S_n^m(e,x_1,\ldots,x_n)} = \lambda v_1, \ldots, v_m(\Phi_e^{n+m}(x_1, \ldots, x_n, v_1, \ldots, v_m)$$

Dôkaz. e – číslo programu P – načítava $n+m$ vstupných hodnôt. P' – program, ktorý miesto načítavanie $x_1, \ldots, x_n$ bude ich mať v sebe zapísané. Potom podľa church tézy to platí.

Veta 9.1.4

(a) *Nech $\Psi \in RF^{(n+m)}$. Potom existuje $g \in VRF^{(n)}$, ktorá pre každé $x_1, \ldots, x_n$ spĺňa $\Phi^{(m)}_{g(x_1,\ldots,x_n)} = \lambda v_1, \ldots, v_m \Psi(x_1, \ldots, x_n, v_1, \ldots, v_m)$.*

(b) *Nech $Q \in ROM^{(n+m)}$ je relácia. Potom existuje taká $g \in VRF^{(n)}$, ktorá pre každé $x_1, \ldots, x_n$ spĺňa $W^{(m)}_{g(x_1,\ldots x_n)} = \{v_1, \ldots, v_m | Q(x_1, \ldots, x_n, v_1, \ldots, v_m\}$.*

Príklad. Totálnosť $Tot =^{def} \{x|\Phi_x$ je totálna $\}$.

Cieľ: ukážeme, že Tot je Π_2-kompletná.

a) $Tot \in \Pi_2$ – $e \in Tot \Leftrightarrow (\forall v)(\exists y)(T(e,v,y) = 0)$

b) Ukážeme, že $(\forall A)(A \in \Pi_2 \Rightarrow A \leq_m Tot)$.

Nech $A \subseteq \mathbb{N}$ je ľubovoľná Π_2 množina.

$A = \{x|(\forall v)(\exists y)R(x,v,y)\}$

$x \in A \Leftrightarrow (\forall v)(\exists y)R(n,v,y)$.

$\Psi(x,v) =^{def} \lambda v(min(y, R(x,v,y))) \in$ČRF

Konštanta $x \in A \to \Psi(x, v)$ je totálna
Konštanta $x \notin A \to \Psi(x, v)$ nie je totálna

$\Psi(x, v) = \Phi_{g(x)}(v)$, t.j. $g(x)$ (je VRF) je index funkcie $\Phi(x, v)$.

$x \in A \Leftrightarrow \Phi_{g(x)}(v)$ je totálna funkcia $\Leftrightarrow g(x) \in Tot$.

Príklad. Niekde definované funkcie.
$B =^{def} \{x | W_x \neq \emptyset\} = \{x | (\exists y) y \in W_x\}$.

a) $B \in \Sigma_1$.

b) $(\forall A \in \Sigma_1)(A \leq_m B)$. Nech A je ľubovoľná ROM. Nech $Q_A =^{def} \{(x, v) | x \in A\} = A \times \mathbb{N}$ Q_A je ROM.

Ak $x \in A \to \{v | (x, v) \in Q_A\} = \mathbb{N}$

Ak $x \notin A \to \{v | (x, v) \in Q_A\} = \emptyset$

$x \in A \Leftrightarrow W_{g(x)} \neq \emptyset$. – dokonči si to $(S - m - n$ veta)

$t.j. A \leq_m B \Rightarrow B$ je Σ_1-kompletná $\Rightarrow B \notin VRM, \bar{B} \notin ROM..$